Harbor Point Hospitality Group

A Threat Intelligence-Driven Solutions Architecture Case Study

Solutions Architecture and Cybersecurity Threat Intelligence Practical Assignment

Justin Goncalves

3/16/2026

Table of Contents

Project Overview:

The objective of this exercise is to simulate a real-world **discovery and solution design engagement**. You will conduct a mock discovery session to assess a customer's operational workflows, technology ecosystem, and threat landscape—then design an architecture that demonstrates how intelligence can be integrated to strengthen their security operations.

Your goal is to:

- Understand the organization's technologies, workflows, and challenges.
- Identify opportunities to integrate threat intelligence effectively.
- Recommend integrations, data flows, and use cases that provide measurable value.

Scenario

During your discovery, focus on understanding the customer's:

- **Operational workflows:** daily processes and cross-team collaboration.
- **Tools and technologies:** including SIEM, SOAR, IAM, and vulnerability management platforms. Remember to include logs and telemetry needed or used.
- **Threat landscape:** types of threats they face, collection sources, and existing detection capabilities.
    - List CTI tradecraft activities the program would perform regularly
- **Incident response approach:** how they currently respond to incidents and leverage intelligence.

Based on this information, propose integrations and use cases where Recorded Future can enhance their capabilities.

Assignment Objectives

1. Select a Customer or Organization (Real or Hypothetical)
Choose a previous customer, employer, or environment you're familiar with to ground your design in reality.

2. Company and Threat Landscape Overview

- Briefly describe the company, industry, and size.
- Summarize key threats relevant to that industry.
- Apply threat profiling to outline possible **threat types, actors, and attack vectors** targeting the organization.

3. Security Organization Layout

- Describe the structure and roles within the security organization. (e.g. SOC, IR, CTI, Engineering, Vulnerability, Network Engineering, IT Help Desk, MSSP, etc.)
    - Which are within normal operations which ones support operations
- Outline how these teams function and collaborate.
- Map out the **operational workflow** uncovered during your discovery (e.g. incident workflow, intel exchange loop, engineering tuning etc.)

4. Current vs. Future State Architecture

- Document the customer's **current security technologies** (e.g. SIEM, EDR, IAM, Vulnerability Management tools).
    - Note: Assume they are using Tines SOAR
- Identify opportunities for improvement and propose a **future state** design.
- Capture any key data flows or technical dependencies critical to your proposed architecture.

5. Data Flow Diagram

Include a visual diagram showing:

- Current-state data ingestion and intelligence flow.
- Proposed future-state architecture integrating Recorded Future and supporting technologies.

6. Integration Recommendations

Provide **two integration suggestions** aligned with the customer's environment. For each:

- Describe the integration and its purpose.
- Explain how it enhances operational efficiency or security posture.
- Highlight key benefits and rationale for prioritization.

7. Recorded Future Use Cases

Present **two specific use cases** demonstrating how Recorded Future intelligence can add value.
For each, include:

- The operational challenge or gap addressed.
- How the use case impacts existing processes.
- The measurable outcomes or benefits to the customer.
- **One use case should pertain to Tines SOAR**
    - Download and setup the community edition and either create your own playbooks or utilize the Recorded Future template playbooks provided by Tines
    - https://www.tines.com/blog/announcing-the-tines-community-edition/
        - We will provide an API token via Virtu (security transfer, please check your email)
- **The second use case** *can* relate to any tool identified in the hypothetical technology stack. We do not expect you to configure this tool like Tines. We expect a hypothetical use case based on reading your selected security tool and Recorded Future's public documentation.
- API usage summary including expected daily API usage per use case. Refer to the Recorded Future API documentation mentioned in Guidelines below.

Guidelines

- You may reference public sources such as **Recorded Future's website**, **GitHub**, **YouTube**, and **partner integration documentation**:
  https://www.recordedfuture.com/integrations/
  https://docs.recordedfuture.com/reference/get-started
- If you use AI tools like ChatGPT, Gemini, etc., highlight where and how you used them throughout this practical.
- The deliverable should be clear, structured, and professional—suitable for presentation for a large group of both sophisticated and an immature audience.
- Feel free to contact us for clarification

Objective 1: Client Selection and Environment Overview

*For the purposes of this assessment, the organization is referred to as **Harbor Point Hospitality Group**, a composite and anonymized hospitality organization based on a real-world environment.*

Client: Harbor Point Hospitality Group

Profile: Composite, anonymized mid-size hospitality organization modeled on a real-world environment

Industry: Hospitality

Locations: Six hotel properties and one corporate office (seven total locations)

Geographic Footprint: Five hotels and the corporate office in the New England region; one hotel location in Michigan

Organization Size: Approximately 400–600 employees total

- 50–100 employees per hotel location
- 50–60 employees at the corporate office

IT & Security Model: Centralized corporate IT and security team responsible for supporting and monitoring all locations

Technology Posture: Hybrid, cloud-first architecture

- A small number of on-premise legacy servers supporting hotel operations, including file services, print services, and property management system (PMS) integrations
- Microsoft 365 used for business productivity and communication
- On-prem Active Directory synchronized to Microsoft Entra ID for identity management
- All endpoints onboarded to Sentinel One EDR
- Security telemetry centralized within Microsoft Sentinel

Security Maturity: Intermediate; foundational controls in place with limited automation and inconsistent operational use of threat intelligence

Objective 2: Company and Threat Landscape Overview

This portion of the assignment builds a clearer picture of Harbor Point Hospitality Group and the security challenges it faces in day-to-day operations. It looks at the organization's industry, size, and distributed environment, and outlines the types of threats most likely to affect it, along with where gaps in visibility and context exist today. Together, this helps establish a realistic risk baseline that informs the architecture, integrations, and use cases explored later in the assessment.

2.1 - Company Profile

Harbor Point Hospitality Group is a mid-size hospitality organization that owns and operates multiple hotel properties supported by a centralized corporate office. The company includes six hotel locations and one corporate headquarters across the United States, with most properties and the corporate office located in the New England region and one additional hotel located in Michigan. In total, the organization employs approximately 400–600 people. A centralized corporate IT and security team is responsible for supporting technology operations and maintaining security oversight across all properties.

From an operational perspective, the corporate IT team based in New England provides both remote and on-site support to the five hotel locations within the region, traveling to individual properties as needed to address infrastructure, endpoint, and network-related issues. The hotel located in Michigan maintains a small local IT presence to handle day-to-day support needs, while coordinating with and escalating to the corporate IT and security team when required. Because physical access to systems is not always immediate, this support model relies heavily on remote access and clear, real-time visibility into system and security activity across all locations.

The organization follows a hybrid, cloud-first approach that balances modern cloud services with a small number of legacy on-premise systems commonly found in hospitality environments. On-premise servers are used to support shared file services, print services, and integrations with vendor-managed systems such as property management platforms. These servers also host Active Directory services that include user accounts for employees across all hotel locations and the corporate office, rather than being separated by property. This centralized identity model, which is common in multi-property hospitality organizations, allows employees to access resources consistently across locations while making identity services a shared dependency across the environment. Business productivity, collaboration, and communication are provided through Microsoft 365, with identities synchronized to Microsoft Entra ID. Security telemetry from endpoints and identity activity is centrally collected and monitored through Microsoft Sentinel, providing unified visibility across the organization.

2.2 - Industry-Relevant Threat Landscape

Hospitality organizations like Harbor Point Hospitality Group operate across multiple locations, support a wide range of employee roles, and depend heavily on identity-based access to both cloud and on-premise systems. Because of this, they are common targets for cyber threats that often start with compromised user accounts, misuse of remote access, or abuse of legitimate credentials. While the organization has foundational security controls in place, the greatest risks tend to come from how attackers take advantage of normal day-to-day workflows to disrupt operations or cause financial impact.

I selected the following threats based on their relevance to the organization's operating model, pre-existing architecture, and distributed environment. They also represent the most likely paths for initial access, lateral movement, and operational impact. While additional threats *do* exist, these areas present the highest risk to the organization's day-to-day operations and security posture.

- **Phishing and Credential Theft**
  Hospitality employees frequently interact with external guests, vendors, and partners, increasing exposure to phishing emails and social engineering attempts. Compromised credentials can provide attackers with access to email, cloud services, and remote access pathways.

- **Identity and Access Abuse**
  Centralized identity services spanning multiple locations increase the risk that compromised or misused accounts can be leveraged to access systems across the environment. Excessive privileges or insufficient access controls can further amplify the impact of identity-based attacks.

- **Abuse of Remote Access Services**
  Remote access solutions used by employees and IT staff are common targets for attackers seeking to bypass perimeter defenses. Stolen credentials, MFA fatigue, or misconfigured access controls can enable unauthorized access without exploiting traditional vulnerabilities.

- **Malware and Endpoint Compromise**
  A diverse endpoint landscape, including front-desk systems, back-office workstations, and operational devices, creates multiple opportunities for malware delivery. Compromised endpoints can be used to establish persistence, collect credentials, or support follow-on attacks.

- **Ransomware Attacks**
  Hospitality organizations remain attractive ransomware targets due to their sensitivity to service disruption and operational downtime. Even when data backups are in place, ransomware incidents can impact endpoints, identity services, and systems critical to guest operations.

2.3 - Threat Profiling: Threat Types, Actors, and Attack Vectors

The threats most relevant to the hospitality industry are typically driven by financially motivated and opportunistic attackers, rather than highly sophisticated or targeted adversaries. These attackers tend to look for environments where access can be gained with minimal resistance and where disruption or financial pressure can be applied quickly. Organizations with multiple locations, a large user base, and shared identity systems often fall into this category, especially when attackers are able to gain legitimate access without immediately raising any red flags.

In practice, attacks in environments like this usually start in fairly routine ways. Phishing emails, social engineering, and other tactics aimed at stealing user credentials are common entry points. Once credentials are compromised, attackers often sign in through normal channels such as email, cloud portals, or remote access tools instead of exploiting technical flaws. In some cases, malware is introduced through malicious links or attachments, allowing the attackers to maintain access or gather additional credentials. Because these actions closely resemble everyday user behavior, early activity can blend into normal operations and go unnoticed without sufficient context.

After gaining access, attackers typically rely on the same identity systems and access paths used by normal employees to move laterally and horizontally throughout the environment. Centralized identity services and shared access across locations can sometimes allow a single compromised account to be used more broadly than intended. Endpoint access may then be leveraged to maintain persistence or prepare for wider disruption. In many cases, attackers focus on creating operational impact, such as service outages or system downtime, knowing that even short disruptions can cause immediate financial and reputational damage and place pressure on the victim to respond quickly. However, not all attackers immediately seek disruption. Some attempt to remain undetected for extended periods, particularly when their goal is financial fraud, credential harvesting, or data theft. In these situations, attackers may limit their activity to email, identity systems, and cloud services, avoiding noisy behavior until their objective is achieved or access is no longer needed.

2.4 - Intelligence Gaps and Risk Exposure

Despite having foundational security controls and centralized monitoring in place, Harbor Point Hospitality Group still faces several intelligence-related gaps that affect its ability to quickly understand, prioritize, and respond to security events. These gaps are less about a lack of alerts and more about limited context, slower and weaker decision-making, and the inconsistent use of existing intelligence during investigations and incident response efforts. Altogether, they increase the organization’s exposure to both disruptive attacks and stealthy misuse of legitimate access.

The following intelligence gaps represent the most significant areas of risk given how the organization operates and the types of threats it is most likely to face.

- **There is limited context when something looks *suspicious***

  Alerts and logs can show that something unusual is happening, but they don't always explain whether an IP address, domain, or file is actually dangerous. As a result, analysts often have to look things up manually or make judgment calls with incomplete information, which slows investigations and can lead to the wrong level of triage and/or response.

- **It is hard to tell normal user activity from stolen credentials**

  Many attacks use valid usernames and passwords, which makes them difficult to spot early. Without strong intelligence context, suspicious sign-ins or endpoint activity can look very similar to normal employee behavior and may go unnoticed longer than they should.

- **They have reactive responses as opposed to proactive efforts**

  The organization has limited ability to block or stop known malicious infrastructure before it causes impact. In many cases, action begins only after alerts fire or systems are already affected, giving attackers more time to move around and prepare for disruption.

- **Threat intel is not used consistently across investigations**

  Intelligence is not always built into everyday investigative workflows, so how it gets used can depend on the analyst or the situation. This leads to uneven investigations, slower response times, and missed opportunities to apply lessons learned from previous incidents.

Objective 3: Security Organization Layout

This section explored how IT and security work were organized and executed in practice at Harbor Point Hospitality Group. I focused on the roles involved, how responsibilities overlapped across teams, and how issues flowed from detection to response. Understanding these real-world workflows helped highlight where improvements in intelligence, automation, and integration would have the most practical impact.

3.1 - Structure and Roles

Harbor Point Hospitality Group relies on a centralized corporate IT team to support technology and security operations across all hotel locations and the corporate office. Given the organization's size and distributed operating model, responsibilities are not strictly separated, and many functions overlap between IT operations and security. Core infrastructure, networking, and firewall management are supported by a managed service provider, with escalation paths in place for higher-impact or specialized issues.

Security Operations

- A small centralized corporate IT team is responsible for day-to-day IT operations as well as security monitoring across all locations.
- Team members wear multiple hats, handling endpoint support, identity management, alert review, and security-related issues as part of their normal workload.
- Security alerts and activity are reviewed through centralized tools rather than a dedicated, around-the-clock security operations center.
- The emphasis is on maintaining visibility and responding to issues that have real operational impact, rather than running a traditional SOC model.
- Standard operating procedures (SOPs) and internal playbooks are used to guide routine tasks, troubleshooting, and common security scenarios, to help maintain consistency despite the fact that there are overlapping responsibilities.

Incident Response

- Initial investigation and response activities are handled by the corporate IT team when alerts, suspicious activity, or user-reported issues arise.
- The same team is responsible for triage, scoring impact/risk/priority, and deciding on containment or escalation steps.
- Response efforts are largely reactive, driven by alerts from existing tools, user reports, or observed system behavior.
- For incidents involving network, firewall, or infrastructure changes, the managed service provider assists as needed.

Threat Intelligence

- Threat intelligence is not managed by a dedicated team or formal intelligence program.
- Intelligence gathering is performed manually and on an ad-hoc basis, depending on individual experience, familiarity with threats, and the specific investigation.
- The same staff handling alerts and incidents also perform intelligence-related research when needed.
- Intelligence is primarily used to answer practical questions during investigations, such as whether an indicator is credible or how urgent a response should be.
- As a result, threat intelligence context/application varies depending on who is handling the issue and what information is immediately available.

Network Engineering and Infrastructure

- Network engineering and infrastructure responsibilities are primarily handled by the managed service provider.
- This includes network configuration, firewall management, and support for on-premise systems.
- The corporate IT team maintains oversight and coordination, while the MSP executes changes and handles specialized tasks.
- During security incidents, the MSP may assist with containment actions such as firewall rule changes or network isolation.

Vulnerability and Endpoint Management

- Vulnerability and endpoint management are handled internally by the corporate IT team.
- Activities such as patching, endpoint protection, and configuration management are part of routine maintenance and operational work.
- Vulnerabilities are prioritized based on risk and operational impact rather than through a formal vulnerability management program.
- Higher-risk issues are escalated through incident response or change workflows when necessary.

IT Help Desk and Local Support

- Day-to-day user support is primarily handled by the corporate IT team for all hotel locations.
- The hotel located outside the primary operating region maintains a small local IT presence to support on-site operational needs.
- Common issues such as workstation problems, basic access requests, and device troubleshooting are handled centrally when possible, with local IT assisting where physical presence is required.
- Security-related concerns or issues outside normal support are escalated to the corporate IT team.
- This approach allows the organization to maintain centralized oversight while still addressing location-specific needs when physical access is required.

3.2 - Operational Workflow and Team Collaboration

At Harbor Point Hospitality Group, IT and security work are handled together rather than as completely separate functions. Issues are brought to the attention of the IT staff in a few different ways: users call or email to submit tickets for everyday IT problems, alerts are generated by monitoring tools such as Microsoft Sentinel or endpoint protection, or something unusual is noticed during routine day-to-day work. ServiceNow, which serves as the central ticketing system for the organization, is used to document issues and resolutions, assign ownership of tickets, and determine next steps. The corporate IT team reviews incoming tickets and alerts, decides whether a security concern is involved, and begins investigating when necessary. Investigations typically focus on identity activity, endpoint behavior, and basic log review, guided by existing SOPs and playbooks. Identity systems often serve as the common thread across investigations, linking user access, endpoint activity, and cloud services. Threat intelligence may be referenced to help gauge risk or urgency, but it is used manually and only when it adds value to the situation at hand.

When additional support or escalation is required, collaboration happens through a combination of ServiceNow workflows and direct communication. The corporate IT team remains responsible for coordinating the response, while the managed service provider is engaged for network, firewall, or infrastructure-related tasks. If physical access or on-site assistance is needed, the local IT staff at the Michigan location, or corporate IT personnel, can travel on-site as needed. Throughout the ticket/incident lifecycle, ServiceNow is the main system of record and documentation, capturing actions taken, any communications both internally and externally, decisions made, and any escalation that occurs. Findings from investigations or recurring issues are informally fed back into configuration changes, alert tuning, or procedural updates, typically handled by the same staff responsible for daily operations. While this approach works well for a lean organization and keeps operations moving, response speed and consistency depend heavily on manual effort, individual judgment, and how quickly meaningful context can be gathered across multiple tools.

Objective 4: Current vs. Future State Architecture

In Objective 4, I examined Harbor Point Hospitality Group's current security architecture and how it could realistically evolve over time. I documented the tools and platforms in place at the time of discovery, identified where gaps in context, coordination, and timing created friction during investigations, and outlined a future state designed to better connect intelligence, automation, and response. The intent of this section was to show how the existing architecture could be strengthened without adding unnecessary complexity, while remaining aligned with how the organization already operated

4.1 - Current State Security Architecture

Harbor Point Hospitality Group's current security architecture is built around a small number of core platforms that support identity, endpoint protection, monitoring, and incident tracking across a distributed environment. These tools provide baseline visibility and protection, but they operate fairly independently, with most correlation, prioritization, and decision-making handled manually by the corporate IT team.

IAM (Identity and Access Management)

- Identity and access are managed through Microsoft Entra ID, which handles user authentication, access control, and sign-in logging.
- Identity logs and sign-in activity are available for review but are primarily used reactively during investigations.
- There is no automated intelligence-driven risk scoring or proactive response tied to identity events.

EDR (Endpoint Detection and Response)

- Endpoint protection and detection are provided by SentinelOne across corporate and hotel systems.
- Endpoint alerts are generated based on behavioral and signature-based detections.
- Alerts are reviewed manually and investigated alongside other signals when they surface.

SIEM (Security Information and Event Management)

- Microsoft Sentinel is used as the centralized SIEM for collecting and reviewing security logs.
- Sentinel ingests data from identity systems, endpoints, and cloud services.
- Alert review and triage are handled manually by the corporate IT team, without dedicated SOC staffing.

Incident Response and Ticketing

- ServiceNow is used as the primary system for both IT tickets and security-related incidents.
- Incidents are created based on alerts, user reports, or observed issues.
- Enrichment, prioritization, and context gathering are performed manually during the investigation process.

Network and Infrastructure Security

- Network infrastructure and firewall management are supported by a managed service provider.
- Firewall rules and network changes are typically made in response to identified issues or incidents.
- Decisions around blocking traffic or making security-related network changes typically involve manual review and coordination between corporate IT and the MSP.

SOAR (Security Orchestration, Automation and Response)

- The organization is assumed to have Tines available as a SOAR platform.
- Currently, automation is limited, and most workflows depend on manual investigation and decision-making.
- Security actions, enrichment, and escalation are largely driven by human effort rather than automated logic.

Backups and Recovery

- File servers and shared resources are backed up on a regular basis to support recovery from data loss, system failure, or operational disruption.
- Backups are primarily focused on maintaining business continuity rather than serving as a security control.
- Recovery activities are typically handled by the corporate IT team, with assistance from the managed service provider when infrastructure or server-level restoration is required.

4.2 - Opportunities for Improvement

While Harbor Point Hospitality Group has a solid set of foundational security controls in place, there are clear opportunities to improve how security information is gathered, understood, and acted on in day-to-day operations. The gaps are not about a lack of tools, but about how context is applied, how consistently intelligence is used, and how quickly decisions can be made during an investigation. Improving these areas would reduce the amount of manual effort required from staff and help the organization move away from purely reactive response toward earlier, more confident action.

- **Improve access to actionable threat context during investigations**

  Alerts and logs often indicate that something unusual is happening, but they do not always provide enough context to quickly determine whether the activity is actually malicious. As a result, analysts frequently have to pause and research indicators on their own. Providing clearer, risk-based context alongside alerts would make it easier to prioritize issues and reduce time spent chasing low-risk activity.

- **Better distinguish legitimate activity from credential misuse**

  Many investigations involve valid user accounts and normal access paths, which makes early signs of compromise harder to spot. Without stronger context tied to identity behavior, endpoints, and

external infrastructure, suspicious activity can blend in with everyday usage. Improving visibility in this area would help surface misuse sooner, even when no obvious technical exploit is present.

- **Shift from reactive response to proactive disruption**
  Most response actions today begin only after alerts fire or systems show signs of impact. This gives attackers more time to move around and prepare follow-on actions. Introducing the ability to proactively block or disrupt known malicious infrastructure would help reduce attacker dwell time and limit the likelihood of broader disruption.

- **Standardize how intelligence is used across workflows**
  Threat intelligence is currently used in different ways depending on who is handling the issue and how much time is available. This leads to uneven investigations and inconsistent outcomes. Making intelligence a more natural part of everyday workflows would improve consistency, reduce analyst fatigue, and make it easier to apply lessons learned across incidents.

- **Reduce manual effort through targeted automation**
  Many investigative steps involve repetitive tasks such as enrichment, documentation, and coordination between teams. Automating these supporting actions would allow staff to spend less time on manual work and more time on analysis and decision-making, while also improving overall response speed.

4.3 - Proposed Future State Security Architecture

To improve upon its current state of security architecture, Harbor Point Hospitality Group does not need to replace its existing security tools, but instead improve how intelligence, automation, and workflows are connected throughout the environment. The focus will be placed on getting *better* context *earlier*, reducing manual effort, and making response actions more *consistent* across identity, endpoint, and network security. This approach supports the organization's existing operating model, while reducing exposure to both disruptive attacks and stealthy misuse of legitimate access.

The future state security architecture focuses on the following areas:

1. **Intelligence-driven investigations**
   • Security alerts and incidents are automatically enriched using Recorded Future API lookups, providing risk scores, criticality, supporting evidence, and related infrastructure context at the time of investigation.
   • Enrichment results are surfaced directly within Microsoft Sentinel and ServiceNow, allowing analysts to quickly assess relevance and severity without performing manual external research.
   • This approach ensures investigations are guided by intelligence-backed context rather than raw alerts alone.

2. **Identity as an early control point**
   • Identity telemetry is treated as an early indicator of risk rather than a signal reviewed only after escalation.
   • Identity-related events such as suspicious sign-ins, anomalous access patterns, or exposed credentials are evaluated using intelligence-driven context to determine potential threat relevance.
   • When elevated risk is identified, predefined response actions can be initiated, including access restrictions, step-up authentication, or escalation into investigation workflows.

3. **Earlier disruption of known malicious infrastructure**
   • High-confidence indicators identified through Recorded Future intelligence, including malicious IPs, domains, and URLs, are evaluated early in the detection lifecycle.
   • Intelligence-backed indicators can trigger targeted containment or blocking actions through existing security and network controls.
   • Blocking decisions are informed by risk scores and confidence levels to minimize operational disruption while reducing exposure to known threats.

4. **Targeted automation to improve consistency**
   • Repetitive investigation tasks such as enrichment, prioritization, ticket creation, routing, and documentation are automated using Tines and intelligence-driven logic.
   • Recorded Future risk scores and intelligence attributes are used as decision points within automation workflows to ensure consistent triage and escalation.
   • This reduces analyst workload while ensuring investigations follow standardized, repeatable response patterns.

5. **Continued alignment of roles across integrated tools**
   • Microsoft Sentinel remains the primary platform for detection, monitoring, and security visibility.
   • ServiceNow continues to serve as the system of record for incident tracking, ownership, escalation, and resolution.
   • Recorded Future intelligence is consumed via API across these platforms to enhance decision-making without altering tool ownership.
   • The managed service provider continues to support network and infrastructure changes when intelligence-backed containment actions are required.

Overall, this would improve how Harbor Point Hospitality Group identifies and responds to security issues without overcomplicating existing workflows. By adding better context earlier and reducing the amount of manual work required during investigations, the team can make faster and more confident decisions. Just as important, these changes fit the way the organization already operates, making them practical to adopt while still reducing risk across a distributed hospitality environment.

Objective 5: Data Flow and Operational Visibility

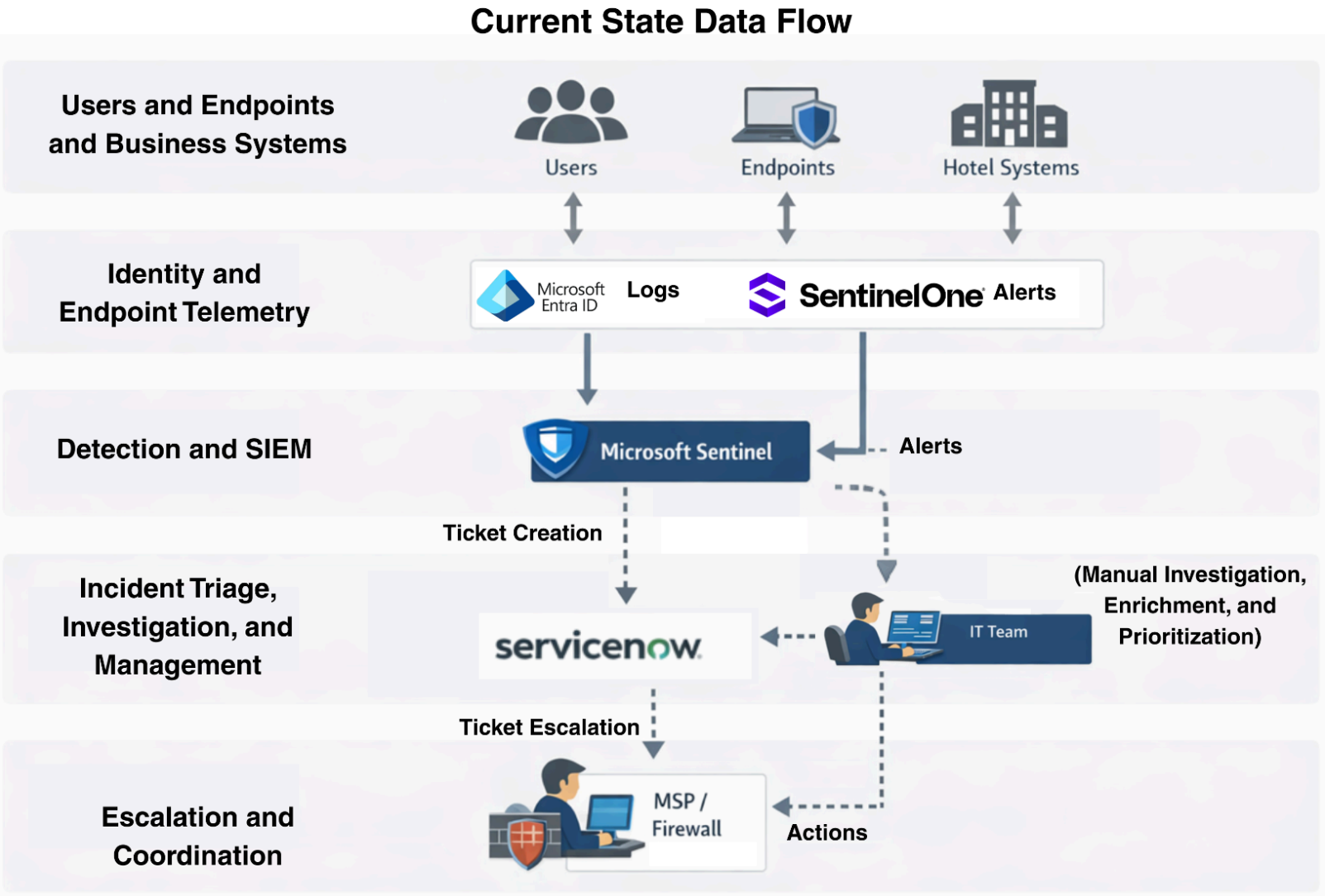
This section illustrates how security data, alerts, and response actions currently move through Harbor Point Hospitality Group's environment, and how those flows would evolve in a future state. The diagrams below are intended to provide a visual representation of the operational reality described in earlier sections, highlighting where manual effort exists today and where improved context, intelligence, and coordination could strengthen detection and response.

5.1 – Current State Security Data Flow

The current state data flow reflects a very reactive security model, where identity and endpoint telemetry are collected across distributed systems and centralized within Microsoft Sentinel for visibility. Alerts and events are manually reviewed by the corporate IT team, with enrichment, prioritization, and investigation performed through a combination of Sentinel, ServiceNow, and external research. Escalation to the managed service provider typically occurs only after manual analysis identifies a need for network or firewall action.

See Visual Diagram Below

Figure 1

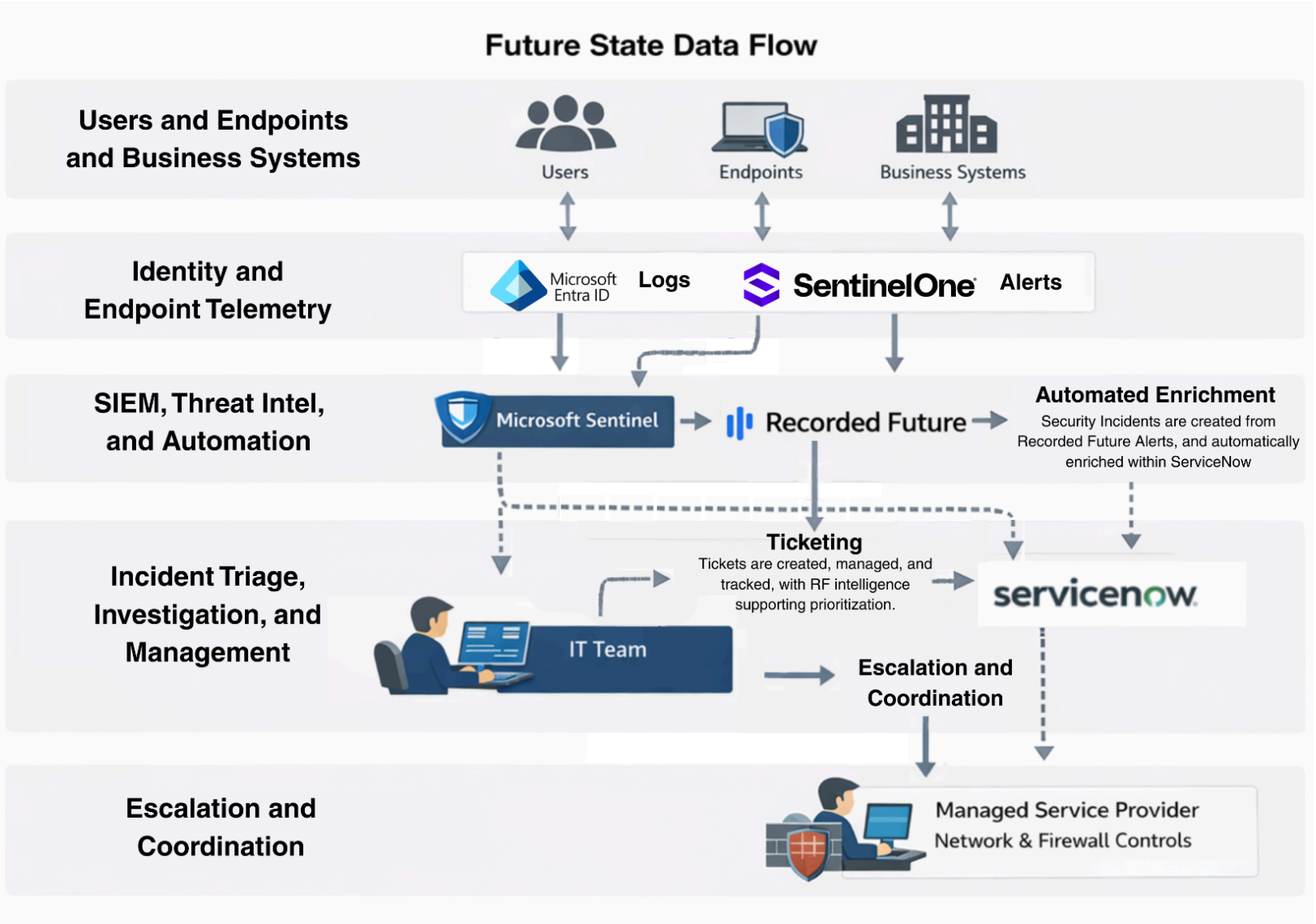


5.2 – Future State Security Data Flow

The proposed future state builds on the existing toolset while improving how security intelligence, automation, and workflows are connected. In this model, identity and endpoint telemetry continue to feed centralized detection, but are bolstered with external threat intelligence to provide earlier context and more confident prioritization. Incidents are enriched automatically, ticketing is guided by intelligence-driven context, and escalation is more deliberate, improving coordinated response actions between corporate IT and the managed service provider.

See Visual Diagram Below

Figure 2


Future State Data Flow
Users and Endpoints and Business Systems
Users
Endpoints
Business Systems
Identity and Endpoint Telemetry
Microsoft Entra ID
Logs
SentinelOne
Alerts
SIEM, Threat Intel, and Automation
Microsoft Sentinel
Recorded Future
Automated Enrichment
Security Incidents are created from Recorded Future Alerts, and automatically enriched within ServiceNow
Incident Triage, Investigation, and Management
Ticketing
Tickets are created, managed, and tracked, with RF intelligence supporting prioritization.
servicenow
IT Team
Escalation and Coordination
Escalation and Coordination
Managed Service Provider
Network & Firewall Controls

Objective 6: Integration Recommendations

In previous objectives, I was able to identify several opportunities and areas for improvement within Harbor Point Hospitality Group, to optimize its workflows, increase efficiency, and harden their security posture. In Objective 6, I list 3 recommendations for integrations with the Recorded Future platform, to strengthen security operations without introducing unnecessary complexity. The following recommendations focus on integrating intelligence directly into the tools and workflows the organization already relies on, with the goal of improving prevention, investigation quality, and response consistency. Each integration was selected based on its ability to reduce manual effort, close the previously identified intelligence gaps, and deliver measurable security value within a lean, centralized IT and security operating model.

6.1 - SentinelOne + Recorded Future, Threat Prevention Integration

Integration Overview and Purpose

This integration connects Recorded Future threat intelligence with SentinelOne to strengthen Harbor Point Hospitality Group's ability to proactively prevent known malicious activity before it impacts endpoints or hotel operations. By feeding Recorded Future RiskLists and Security Control Feeds into SentinelOne, the organization can automatically block high-confidence malicious IPs, domains, and file hashes that are actively being used by attackers.

Instead of relying only on endpoint behavior after something has already executed, this approach adds outside context to SentinelOne's existing XDR capabilities. When intelligence shows that infrastructure is clearly malicious, SentinelOne can prevent communication or execution up front, reducing exposure to common threats like ransomware delivery, malware staging, and command-and-control traffic.

The primary goal of this integration is to move security controls upstream in the attack lifecycle. Rather than waiting for suspicious behavior to trigger alerts and investigations, the organization gains the ability to deny known bad infrastructure at the endpoint and network level, reducing exposure to common threats such as ransomware, malware delivery, and command-and-control activity.

Operational and Security Impact

In the current state, blocking decisions are largely reactive and require manual analysis, coordination, and execution. This integration reduces that dependency by allowing SentinelOne to continuously consume Recorded Future RiskLists and Security Control Feeds and enforce preventative controls automatically.

By applying external intelligence directly within SentinelOne, the IT team no longer needs to manually research indicators before taking action. High-confidence indicators can be blocked consistently across endpoints, while lower-confidence indicators can still be reviewed and handled through existing investigation workflows. This approach improves response speed without sacrificing control or operational stability.

Key Benefits and Rationale for Prioritization

This integration is prioritized because it delivers immediate risk reduction with minimal operational overhead. Hospitality environments are highly sensitive to downtime, and preventing known malicious activity early helps reduce the likelihood of disruptive incidents that could affect guest services, hotel operations, or revenue-generating systems.

Key benefits include:

- Reduced reliance on manual indicator analysis and blocking decisions
- Earlier prevention of known malicious infrastructure at the endpoint level
- Consistent application of threat intelligence across the environment
- Lower risk of ransomware, malware infections, and lateral movement
- Improved security posture without adding complexity to existing workflows

By focusing on prevention rather than investigation alone, this integration directly addresses one of the organization's most significant gaps identified in the current state and supports a more resilient, intelligence-driven security model.

6.2 - ServiceNow + Recorded Future, Threat Intelligence Integration

Integration Overview and Purpose

This integration connects Recorded Future threat intelligence directly into ServiceNow IT Service Management (ITSM) and Security Incident Response (SIR), ensuring that external intelligence is available within the system where incidents are already tracked, investigated, and resolved. The primary purpose of this integration is to improve investigation quality, prioritization, and consistency by embedding threat context directly into existing incident workflows.

Rather than requiring analysts to pivot between multiple tools to validate indicators or assess risk, ServiceNow can automatically query Recorded Future for relevant intelligence as incidents are created or updated. This allows responders to quickly understand the significance of an indicator and make informed decisions without leaving the platform they already rely on.

How It Improves Operations and Security

ServiceNow currently serves as the system of record for operational and security-related incidents, but much of the investigative context is gathered manually. By integrating Recorded Future, security incidents can be automatically enriched with risk scores, supporting evidence, and related threat information directly within ServiceNow SIR.

In addition to enrichment, high-confidence alerts generated by Recorded Future can be used to automatically create security incidents in ServiceNow. This ensures that intelligence-driven findings are consistently tracked, assigned, and managed through established processes, reducing the likelihood that critical

threats are overlooked or delayed.

This integration also supports the ingestion of ongoing threat intelligence observables into ServiceNow, providing a continuously updated intelligence foundation that strengthens investigations over time. Together, these capabilities reduce manual effort, improve triage accuracy, and create a more consistent investigative experience across both IT and security teams.

Key Benefits and Rationale for Prioritization

This integration is prioritized because it enhances security operations without disrupting existing workflows or introducing new tools. By delivering intelligence directly into ServiceNow, Harbor Point Hospitality Group can improve both speed and confidence during incident response while maintaining a centralized operating model.

Key benefits include:

- Faster and more consistent triage by embedding intelligence directly into existing incident workflows
- Reduced manual effort by eliminating repetitive lookups and external research
- Improved decision-making through risk-based context that supports accurate prioritization
- Better cross-team visibility by aligning security investigations with IT ticketing processes

By embedding threat intelligence into the platform where incidents are already managed, this integration directly addresses identified intelligence gaps and strengthens the organization's ability to respond effectively to security events in a hospitality environment with many properties.

6.3 - Entra ID + Recorded Future, Identity Intelligence Integration

Integration Overview and Purpose

This integration brings Recorded Future Identity Intelligence directly into Microsoft Entra ID (Azure Active Directory) to strengthen Harbor Point Hospitality Group's ability to detect and respond to compromised credentials before they are abused. By continuously monitoring for exposed or compromised identities across open sources, dark web markets, and malware infrastructure, Recorded Future provides early visibility into identity-based threats that may not yet appear in traditional sign-in logs.

The purpose of this integration is to treat identity as an early control point rather than a signal that is only reviewed after suspicious activity occurs. When high-risk credentials are identified, the organization can take targeted action within Entra ID to reduce risk while maintaining operational continuity.

How It Improves Operations and Security

In a distributed hospitality environment, identity misuse is a common and difficult attack vector to detect early. Valid credentials often allow attackers to blend in with normal user behavior, delaying detection and increasing the likelihood of lateral movement or data access.

With this integration in place, Recorded Future automatically surfaces identity compromise intelligence into Entra ID, where it can trigger predefined remediation workflows. At-risk users can be placed into specific security groups, which then apply conditional access policies such as access restrictions, forced authentication challenges, or automated credential resets. These actions can be tailored based on risk level and business impact, ensuring that responses are proportional rather than disruptive.

At the same time, actions taken through Entra ID can be logged and forwarded to Microsoft Sentinel, preserving visibility and ensuring identity-related activity is included in broader security investigations and reporting.

Key Benefits and Rationale for Inclusion

- Earlier detection of compromised credentials before misuse escalates
- Automated, policy-driven identity remediation without manual research
- Risk-based access control using existing Entra ID conditional access policies
- Improved visibility into identity threats through Sentinel logging and correlation
- Stronger alignment between identity security and broader security operations

This integration is included as a strategic, supporting use case because identity is a foundational layer across Harbor Point Hospitality Group's environment. Incorporating external identity threat intelligence reinforces a layered defense strategy and increases protection against one of the most common initial access methods used by attackers.

Objective 7: Recorded Future Use Cases

In previous objectives, I was able to identify several opportunities and areas for improvement within Harbor Point Hospitality Group, to optimize its workflows, increase efficiency, and harden their security posture. In Objective 6, I list 3 recommendations for integrations with the Recorded Future platform, to strengthen security operations without introducing unnecessary complexity. The following recommendations focus on integrating intelligence directly into the tools and workflows the organization already relies on, with the goal of improving prevention, investigation quality, and response consistency. Each integration was selected based on its ability to reduce manual effort, close the previously identified intelligence gaps, and deliver measurable security value within a lean, centralized IT and security operating model.

7.1 - IOC Enrichment, and Automatic ServiceNow Ticket Creation (Tines)

Overview

This use case demonstrates how Recorded Future threat intelligence is operationalized using Tines to support consistent, risk-based investigation and incident handling. The automation ingests indicators of compromise (IOCs)—including file hashes, domains, and IP addresses—via a centralized webhook, enriches them using the Recorded Future API, and applies deterministic decision logic to control escalation, notification, and ticket creation.

Rather than treating every IOC as an incident, the workflow enforces intelligence-driven thresholds that determine whether an indicator warrants analyst awareness, automated escalation, or no further action. By combining webhook-based ingestion, API-driven enrichment, and structured risk gating, the automation reduces alert noise, standardizes triage decisions, and ensures ServiceNow incidents are created only when justified by threat severity.

Workflow Summary

The automation begins when an IOC is submitted to a Tines webhook from an upstream source such as a SIEM, EDR platform, or manual analyst input. The webhook payload includes the IOC type, IOC value, and submission context, providing a consistent ingestion mechanism regardless of source.

Upon ingestion, trigger actions route execution based on IOC type (hash, domain, or IP), ensuring each indicator follows the appropriate enrichment path. For each branch, Tines issues an HTTP request to the corresponding Recorded Future API endpoint to retrieve risk-scored intelligence, including criticality, risk score, summary context, and a direct link to the Recorded Future intelligence card. The raw API response is then normalized into a compact internal object, allowing downstream logic to reference consistent fields regardless of IOC type. Known-good or unfound indicators are filtered early in the workflow, with optional analyst notification, and no further action is taken.

For indicators found in Recorded Future, the workflow applies a tiered risk threshold gate:

- **Critical indicators** automatically generate Priority 1 Security Incidents in ServiceNow
- **High-risk indicators** generate Priority 2 Security Incidents
- **Moderate-risk indicators** trigger automated analyst notification via email without creating a ServiceNow ticket
- **Low-risk indicators** result in lookup visibility only, with no escalation

Challenges Addressed

Prior to automation, IOC validation required analysts to manually query multiple tools, interpret intelligence context, and make subjective escalation decisions. This process introduced delays, inconsistency, and unnecessary ticket creation, particularly for low-confidence indicators. Additionally, the absence of standardized thresholds meant response outcomes varied depending on the individual handling the investigation.This automation replaces ad hoc decision-making with structured, policy-driven logic that enforces consistent outcomes while preserving analyst visibility and control.

Measurable Outcomes and Benefits

- Reduced manual enrichment and validation effort
- More consistent triage and prioritization across analysts
- Fewer low-risk indicators escalated unnecessarily
- Faster creation of high-confidence security incidents
- Improved alignment between threat severity and response urgency
- Increased analyst efficiency without loss of visibility

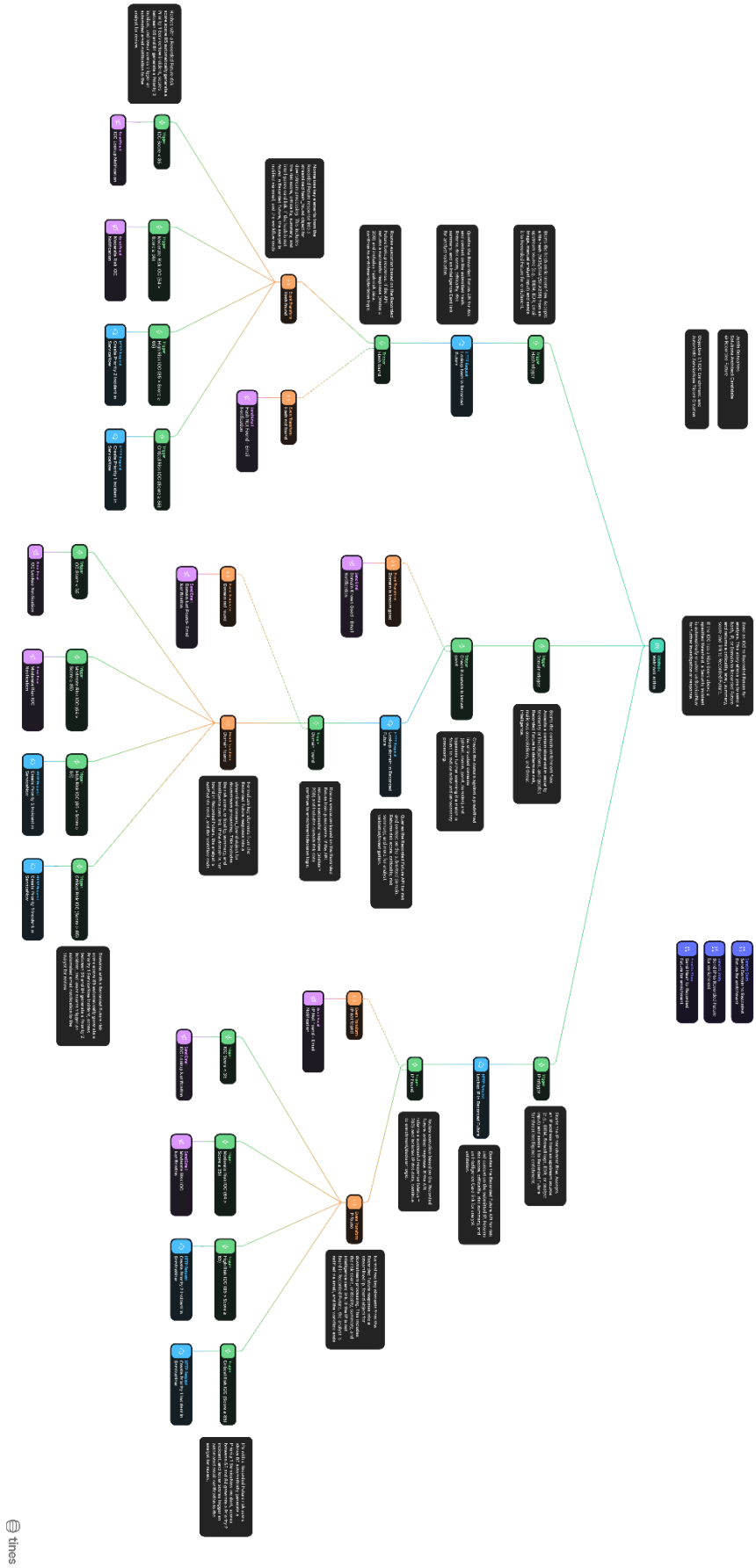
API Usage Summary

This use case relies on on-demand Recorded Future API lookups initiated via webhook-triggered workflows. Each IOC submission results in a single enrichment request to the appropriate Recorded Future endpoint (hash, domain, or IP). No bulk polling, scheduled ingestion, or continuous synchronization is performed.

Based on expected IOC volume from endpoint alerts, SIEM detections, and analyst-driven submissions, estimated API usage for this automation is approximately 100–200 calls per day. API consumption scales linearly with alert volume and is further optimized through early filtering, known-good checks, and risk-based gating, ensuring efficient and controlled use of Recorded Future intelligence.

See Visual Diagram Below

Figure 3: Tines Automation Workflow



7.2 - Microsoft Sentinel + Recorded Future API Integration

Use Case Overview

This use case demonstrates how Recorded Future intelligence can be integrated directly into Microsoft Sentinel to enhance detection fidelity, contextual enrichment, and alert prioritization within a centralized SIEM environment. By ingesting Recorded Future risk-based intelligence into Sentinel as native Threat Intelligence indicators, security teams can correlate external threat context with internal telemetry to identify high-confidence threats more quickly and accurately.

Rather than relying solely on raw log data or static detection rules, this approach enables intelligence-led detection by embedding Recorded Future risk scores, evidence, and confidence into Sentinel analytics. The result is a more informed SOC workflow where alerts are enriched automatically and prioritized based on both internal activity and external threat intelligence.

Workflow Summary

In this use case, Recorded Future intelligence is integrated into Microsoft Sentinel using the official Recorded Future custom connector and Azure Logic Apps. Recorded Future RiskLists and Security Control Feeds are periodically pulled via API and ingested into Sentinel as native Threat Intelligence indicators using Microsoft's Threat Intelligence schema.

These indicators include not only the IOC itself, but also enriched context such as Recorded Future risk scores, confidence levels, evidence, and links back to the Recorded Future Intelligence Card. Once ingested, Sentinel analytic rules and TI mapping templates correlate these indicators against internal telemetry such as firewall logs, endpoint activity, and network traffic.

When correlations occur, Sentinel generates alerts and incidents that are already enriched and scored. Analysts can further trigger enrichment playbooks to pull additional context from Recorded Future directly into the incident, enabling faster investigation and decision-making without leaving the Sentinel console.

Challenges Addressed

In many environments, SIEM detections are generated without sufficient external context, forcing analysts to manually investigate indicators to determine whether they represent real threats or benign activity. This leads to alert fatigue, inconsistent prioritization, and delayed response times—particularly when dealing with indicators such as IP addresses or domains that may appear suspicious but lack immediate confirmation.

Without integrated threat intelligence, organizations struggle to distinguish between low-confidence signals and indicators associated with active command-and-control infrastructure, malicious campaigns, or known adversary activity.

Impact on Existing Security Operations

This integration enhances Sentinel's native detection capabilities by adding intelligence-driven context at multiple stages of the security lifecycle. Alerts are no longer evaluated in isolation; instead, they are assessed using Recorded Future's confidence scoring and historical intelligence.

Detection rules can be tuned to prioritize alerts based on Recorded Future risk score thresholds, allowing SOC teams to focus on high-risk indicators associated with active threats while deprioritizing low-confidence noise. Enrichment playbooks further reduce manual investigation time by automatically attaching risk details and evidence to incidents.

Overall, this approach shifts the SOC from reactive alert handling to proactive, intelligence-informed detection and response.

Measurable Outcomes and Benefits

- Reduced alert fatigue through intelligence-based prioritization
- Faster analyst triage due to automatic IOC enrichment
- Improved detection accuracy by correlating internal telemetry with external threat intelligence
- Consistent, repeatable prioritization based on Recorded Future confidence scores
- Better utilization of Sentinel analytics and existing security telemetry

API Usage Summary

This use case primarily relies on scheduled bulk API interactions rather than per-alert enrichment. Recorded Future RiskLists and Security Control Feeds are retrieved at defined intervals (e.g., hourly for detection-focused lists and daily for prevention-focused feeds) using the Recorded Future API through Azure Logic Apps.

Estimated API usage for this use case is approximately 50–100 API calls per day, depending on the number of feeds enabled and polling frequency. Because indicators are ingested in bulk and reused across multiple detections, API consumption remains predictable and efficient, while still providing continuous intelligence updates.

Conclusion

This assessment illustrates how Recorded Future intelligence can be practically integrated into Harbor Point Hospitality Group's existing security environment to improve prevention, detection, and response without adding unnecessary complexity. By focusing on intelligence-driven workflows, targeted automation, and risk-based prioritization, the proposed architecture strengthens security operations while remaining realistic for a lean, centralized IT and security team supporting a distributed hospitality environment.

Rather than introducing new tools, this approach emphasizes getting more value from the platforms already in place by delivering timely context where decisions are made. The result is a security model that reduces manual effort, improves consistency, and enables earlier, more confident action against meaningful threats. Together, the recommendations and use cases presented form a scalable foundation for intelligence-led security operations that can evolve as the organization and threat landscape continue to grow.

Works Cited

Recorded Future. (n.d.). Recorded Future API documentation: Getting started. https://docs.recordedfuture.com/reference/get-started

Recorded Future. (n.d.). Integrations. https://www.recordedfuture.com/integrations

Tines. (n.d.). Recorded Future × Tines. https://www.tines.com/solutions/products/recorded-future/

Recorded Future. (n.d.). Prevent Account Takeovers: Identity Intelligence by Recorded Future [Video]. YouTube. https://www.youtube.com/watch?v=rBqUpCGFrKA

Recorded Future. (n.d.). Recorded Future Integration with Security Incident Response [Video]. YouTube. https://www.youtube.com/watch?v=jPMSFMYLRNc

Microsoft Events. (n.d.). Intelligence-led security operations in Microsoft Azure Sentinel | (OD438) [Video]. YouTube. https://www.youtube.com/watch?v=t5dBFKT6_Ww

Microsoft Events. (n.d.). Leverage Recorded Future Playbooks to automatically integrate threat intelligence with | OD434 [Video]. YouTube. https://www.youtube.com/watch?v=U_P7HNqhZDQ

Microsoft Security. (n.d.). Recorded Future Identity Intelligence integrates with Microsoft Entra ID (formerly Azure AD) [Video]. YouTube. https://www.youtube.com/watch?v=7NPFT54gsTY

Microsoft Security. (n.d.). Recorded Future Intelligence for Microsoft Sentinel [Video]. YouTube. https://www.youtube.com/watch?v=SNqDsDpcapg